**Amendment to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

Claim 1 (currently amended): A method for generating filters based on data entering a network device, comprising:

separating the data into a plurality of network flows;

creating separate aggregate network flow summaries for each of said network flows;

sending at least one of said aggregate network flow summaries to a flow analyzer at the network device;

analyzing said at least one aggregate network flow ~~summaries~~ summary to detect characteristics of potentially harmful network flows;

generating or refining a filter based on said analyzed aggregate network flow summary to prevent packets corresponding to detected potentially harmful network flows from passing through said network device; and

selecting a new aggregate network flow summary to analyze and sending the selected aggregate network flow summary to the flow analyzer for analysis, wherein the new aggregate flow summary corresponds to a network flow associated with the generated or refined filter.

Claim 2 (canceled).

Claim 3 (currently amended): The method of claim 1 further comprising classifying network flow ~~wherein the network flow is classified~~ based on a source device sending a packet.

Claim 4 (original): The method of claim 3 wherein the network flow is classified based on an IP address of the source device.

Claim 5 (canceled).

Claim 6 (currently amended): The method of claim 1 wherein analyzing said at least one ~~of said network flows~~ aggregate network flow summary comprises monitoring statistics associated with said network flows.

Claim 7 (original): The method of claim 1 further comprising propagating the generated filter to an upstream network device.

Claim 8 (currently amended): The method of claim 1 further comprising sending each of said plurality of network flows to a corresponding flow cache and implementing policies designated for each of said network flows ~~wherein sending each network flow to a corresponding flow cache is performed by hardware and analyzing said network flow is performed by software~~.

Claim 9 (canceled).

Claim 10 (currently amended): The method of claim 1 wherein analyzing said at least one aggregate network flow summary ~~the flow analyzer~~ comprises utilizing software.

Claim 11 (original): The method of claim 1 wherein selecting a new aggregate network flow summary to analyze comprises selecting a class of said network flows to analyze based on previously analyzed network flows.

Claims 12-13 (canceled).

Claim 14 (original): The method of claim 1 wherein detecting potentially harmful network flows comprises identifying a source address associated with said harmful network flow and generating a filter comprises generating a filter to prevent packets from said identified source from passing through said network device.

Claim 15 (currently amended): A computer program product for generating filters based on analyzed network flows, comprising:

code that separates data into different network flows;

code that creates an aggregate network flow summary for one or more of said network flows;

code that selects one or more network flows for analysis;

code that sends said selected aggregate network flow summaries to a flow analyzer at the network device;

code that analyzes said selected network flows by reviewing said aggregate network flow summaries;

code that detects potentially harmful network flows;

code that automatically generates or refines a filter based on said analyzed network flow summary to prevent packets corresponding to said detected potentially harmful network flows from passing through the network device;

code that selects a new aggregate network flow summary to analyze and send the selected aggregate network flow summary to the flow analyzer for analysis; and

a computer-readable storage medium for storing the codes executable by a processor.; ~~wherein the computer-readable storage medium is not a data signal embodied in a carrier wave.~~

Claim 16 (canceled).

Claim 17 (original): The computer program product of claim 15 further comprising code that propagates said filter to an upstream network device.

Claim 18 (previously presented): A system for automatically generating filters based on data entering a network device, comprising:

a netflow device operable to receive streams of packets, separate said streams, and create a summary record containing information on each of said streams;

a flow analyzer located at the network device and operable to receive said summary records from said netflow device and analyze said summary records and identify potentially harmful network flows; and

a filter generator operable to generate or refine a filter based on analyzed summary records to prevent packets corresponding to said identified potentially harmful network flows from passing through the network device, wherein said netflow device is operable to create a new summary record containing information on a stream of data associated with said generated or refined filter.

Claim 19 (original): The system of claim 18 wherein the network device comprises hardware and the flow analyzer and filter generator comprise software.

Claim 20 (original): The system of claim 18 wherein the network device comprises an ACL classifier, a lookup device, and a plurality of flow buckets.

Claim 21 (original): The system of claim 18 further comprising a filter propagator operable to send information on said filters to an upstream device and request the upstream device to create a corresponding filter.

Claim 22 (canceled).

Claim 23 (previously presented): The method of claim 1 wherein information resulting from analyzing at least one of said aggregate network flow summaries is reduced in hardware so that flow records can be analyzed by software.

Claim 24 (previously presented): The method of claim 1 wherein a group of potentially harmful packets is detected and further comprising analyzing said corresponding network flow and further refining said filter.

Claim 25 (previously presented): The method of claim 1 further comprising selecting a group of network flows to be analyzed.

Claim 26 (previously presented): The method of claim 25 further comprising passing information on the selected group of network flows to a classifier.

Claim 27 (previously presented): The method of claim 1 wherein a class of packets to be analyzed is selected based on statistics associated with the generated or refined filter.

Claim 28 (canceled).

Claim 29 (currently amended): The method of ~~claim 28~~ claim 30 wherein each of said filters are generated specifically for a corresponding network flow.

Claim 30 (currently amended): ~~The method of claim 29~~A method for generating filters for network flow, comprising:

receiving data at a network device;

classifying network flows based on one or more packets received at the network device;

analyzing one or more of said network flows;

generating a filter for one or more of said network flows;

processing each of said network flows according to a corresponding policy;

selecting a class of network flows to analyze;

analyzing said selected class of network flows; and

refining said filter for said selected class of network flows, wherein refining said filter comprises modifying the classification of network flows.

Claims 31-34 (canceled).

Claim 35 (previously presented): The system of claim 18 further comprising a netflow directory comprising a plurality of flow cache entries and configured to build new flow cache entries for network flows without a corresponding flow cache entry.

Claim 36 (previously presented): The computer program product of claim 15 further comprising code that refines said filter based on said analyzed network flow.

Claim 37 (previously presented): The method of claim 1 further comprising splitting said filters if traffic into said filter exceeds a sampling capability of the filter.

Claim 38 (previously presented): The method of claim 1 wherein analyzing said aggregate network flow summary comprises analyzing for a specified interval of time.

Claims 39-41 (canceled).

Claim 42 (new): The method of claim 8 wherein sending each of said plurality of network flows is performed by hardware and analyzing said at least one aggregate network flow summary is performed by software.

Claim 43 (new): The system of claim 18 further comprising a classifier operable to classify said streams of packets based on one or more packets received at the netflow device.

Claim 44 (new): An apparatus for generating filters based on analyzed network flows, the apparatus comprising:

one or more processors; and

a memory that stores instructions to be executed by said one or more processors, said instructions comprising:

code that creates separate aggregate network flow summaries for each of said network flows;

code that sends at least one of said aggregate network flow summaries to a flow analyzer at the network device;

code that analyzes said at least one aggregate network flow summary to detect characteristics of potentially harmful network flows;

code that generates or refining a filter based on said analyzed aggregate network flow summary to prevent packets corresponding to detected

potentially harmful network flows from passing through said network device; and

code that selects a new aggregate network flow summary to analyze and sending the selected aggregate network flow summary to the flow analyzer for analysis, wherein the new aggregate flow summary corresponds to a network flow associated with the generated or refined filter.

Claim 45 (new): The apparatus of claim 44 wherein said instructions further comprise code that propagates said filter to an upstream network device.

Claim 46 (new): The apparatus of claim 44 wherein said instructions further comprise code that classifies network flow based on a source device sending a packet.